AFRL-IF-RS-TR-2004-335
Final Technical Report
December 2004

DYNAMIC FAULT AND SECURITY ADAPTIVE OVERLAY NETWORKS (DYNABONE)

USC Information Sciences Institute

Sponsored by
Defense Advanced Research Projects Agency
DARPA Order No. M098

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2004-335 has been reviewed and is approved for publication

APPROVED: /s/
DAVID E. KRZYSIAK
Project Engineer

FOR THE DIRECTOR: /s/
WARREN H. DEBANY, JR.
Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2004	**FINAL** **Jun 01 – Mar 04**

4. TITLE AND SUBTITLE

DYNAMIC FAULT AND SECURITY ADAPTIVE OVERLAY NETWORKS (DYNABONE)

5. FUNDING NUMBERS

G - F30602-01-2-0529
PE - 62301E
PR - FTNP
TA - MO
WU - 98

6. AUTHOR(S)

Joseph Touch, Amy S. Hughes, Yu-Shun Wang, Gregg Finn,
Nimish Kasat, Sun-Hee Yoon, Lars Eggert

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USC Information Sciences Institute
4676 Admiralty Way
Marina Del Rey CA 90292-6695

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Advanced Research Projects Agency
3701 North Fairfax Drive
Arlington VA 22203-1714

AFRL/IFGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

AFRL-IF-RS-TR-2004-335

11. SUPPLEMENTARY NOTES

DARPA Program Manager: Col Timothy Gibson, U.S. Army
AFRL Project Engineer: David E. Krzysiak/IFGA/(315) 330-7454 David.Krzysiak@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 Words)*

Dynamic Fault and Security Adaptive Overlay Networks (DYNABONE) is a system for the rapid configuration, deployment, and management of protective layered overlays, that both proactively and reactively resist Distributed Denial of Service (DDoS) attacks. DYNABONE deploys parallel concurrent "inner" overlays (interlays) and a proactive/reactive multiplexer (PRM) to direct traffic among them. The innerlays are layered and composed into a single "outer" overlay (outerlay) that presents an interface compatible with COTS applications and operating systems. The result is a parallel set of innerlays.

14. SUBJECT TERMS

VPN, overlay, DDoS, fault tolerant, network architecture

15. NUMBER OF PAGES 23

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

List of Figures

1. Overview

DynaBone is a system for the rapid configuration, deployment, and management of protective layered overlays that both proactively and reactively resist distributed denial-of-service (DDOS) attacks. DDOS attacks overload network connections at hosts and routers, often leaving administrators with no solution other than to disconnect the network. DynaBone automates this capability and makes it a viable alternative, by deploying parallel concurrent 'inner' overlays (*innerlays*) and a proactive/reactive multiplexer (PRM) to direct traffic among them. DynaBone uses X-Bone's unique ability to layer and compose these innerlays into a single 'outer' overlay (*outerlay*) that presents an interface compatible with COTS applications and operating systems. The result is a parallel set of innerlays, any subset of which can be disconnected in response to attacks while the outerlay continues to provide effective service over the remaining innerlays. DynaBone's parallelism provides RAID-like defense against failure and attack [10].

This project developed a system for the deployment of multi-level overlays, demonstrating agile reconfiguration of underlying networks without disturbing end-to-end connections. The system demonstrated the performance, scalability, and fault-tolerance of these multilayer networks, proving that highly flexible network architectures can be composed out of layers of Internet overlays. New mechanisms were developed to integrate encapsulation across overlays, which are now being applied to scale both router and bridge architectures. The system also further developed the architecture of a recursive Internet [19][23], with applications to site multihoming, mobility, VPNs, and application-directed networking.

DynaBone investigated the recursive overlay deployment capabilities of the X-Bone, and how best to extend them to support DynaBone overlays. A PRM was designed and a preliminary version implemented in Perl. Parallel concurrent innerlays were deployed using the X-Bone's automated application deployment mechanism [26]. A new technique for resolving tunnel addresses across VPN clouds was developed, called BARP. The X-Bone API was revised and its architecture extended to support DynaBone's recursion. The DynaBone was extended with an open API for PRM control and monitoring, including a graphical user interface (GUI) to that API. The DynaBone was extended to allow arbitrary topologies, and the packet multiplexer was augmented and implemented in-kernel for higher performance. The DynaBone's performance was measured in detail, including both packets/second forwarding rates and bits/second throughput over gigabit Ethernet interfaces. A DynaBone demo included integrated reaction to both in- and out-of-band attacks. Measurement of the impact of IPsec performance on DynaBone overlays was completed. Several beta releases of the code were tested with several collaborators, and a final release was made at the end of Jan. 2004. The final system was tested with over 800 innerlays, up to 16 levels deep. In addition, the TetherNet [17][20] system was completed and is now available to support PI meetings.

2. Progress

The DynaBone system successfully demonstrated that multilevel overlays can support protection against attacks without affecting end-to-end Internet connections, and without requiring new protocols, modifications to operating systems, or modifications to applications. During the project, multilayer overlays as deep as 16 levels, including as many as 800 concurrent innerlays were demonstrated. The system demonstrated reaction to attack, dynamic reconfiguration, and the ability to constrain overlays to specific topologies involving specific nodes. The system was demonstrated on gigabit interfaces, where the packet processing rates were roughly half that of an unmodified system.

2.1 Background

The X-Bone is a system for the dynamic deployment and management of Internet overlay networks [22]. Overlay networks are used to deploy infrastructure on top of existing networks, to isolate tests of new protocols, partition capacity, or present an environment with a simplified topology. The X-Bone system provides a high-level interface where users or applications request DWIM (do what I mean) deployment, e.g.: *create an overlay of 6 routers in a ring, each with 2 hosts*. The X-Bone automatically discovers available components, configures, coordinates their sharing of network components, and monitors deployed overlays.

The X-Bone is a distributed system composed of Resource Daemons (RDs) and Overlay Managers (OMs) , with a graphical user interface (GUI) and a direct API, shown in Figure 1. Further details on the X-Bone are available elsewhere [18].

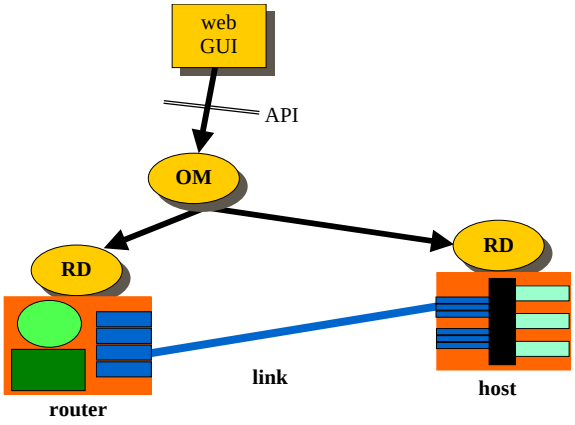

Figure 1. Components of the X-Bone architecture

The DynaBone utilizes the X-Bone architecture to deploy a set of inner overlays (innerlays) together with a feedback and distribution proactive/reactive multiplexer (PRM), layered inside an outer overlay (outerlay). The result is a system of overlays that endures DDOS attacks, because an attack on any individual network can result in its being disconnected without substantially affecting the overall connectivity of the group (Figure 2). When the innerlays of a DynaBone are attacked, its PRM shifts traffic to the unaffected overlays. Further details on the DynaBone architecture are available in published papers [21].

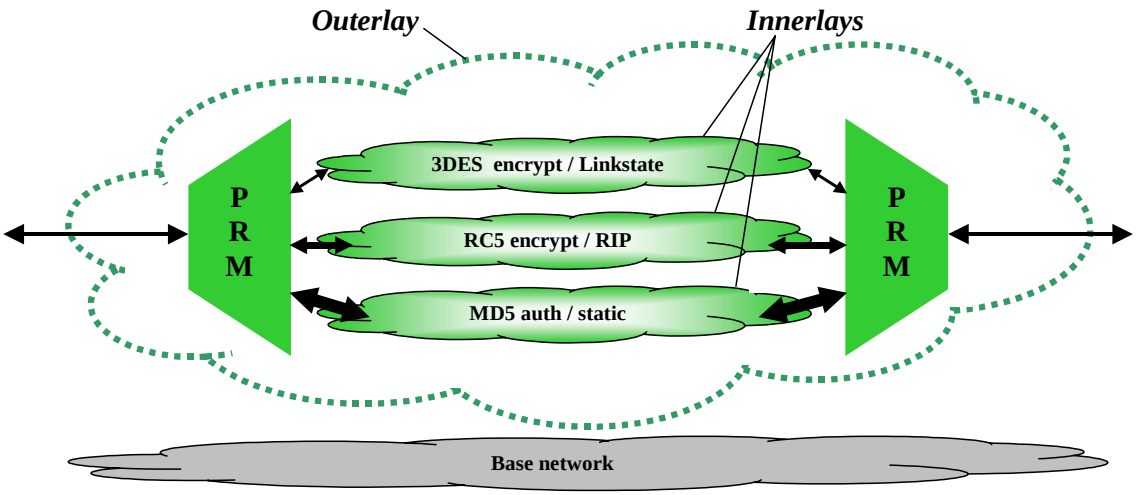

Figure 2. Components of the DynaBone architecture

2.2 Specific Achievements

In addition to accomplishing the desired project objectives, the DynaBone project made several significant discoveries. A new solution to provide cross-cloud address resolution was developed called BARP. The X-Bone architecture was extended to support recursive overlays, including modifications to its APIs and internal architecture. An in-kernel configurable packet multiplexer was also developed.

Address resolution across subordinate VPN clouds (BARP)

The PRMs use the innerlays as transit networks. This is reminiscent of both the way in which IP networks use LANs, and the way in which they use transit autonomous systems (AS's). IP packets transit a LAN using link encapsulation, and discover the link address of the egress using ARP (in IPv4; in IPv6, a slightly modified but nearly equivalent system is used) [3][12][13] . IP packets transit an AS using BGP [14] tables indicating the egress destination, but do not use encapsulation.

In ARP, link layer egress addresses are discovered using broadcast. Given an IP egress address, a local ARP table (cache) is consulted; missing entries are resolved via sending a broadcast request and waiting for a response. This exchange occurs at the time the table is consulted. In BGP, a separate unicast protocol is used to exchange announced egress information.

The DynaBone needs a combination of these two mechanisms. It would be useful to use a separate unicast protocol to gather announced PRM egress addresses, but these addresses are used for encapsulation at the ingress PRM, to traverse the innerlays. For example, in Figure 3, a packet from X to Y arrives at X's PRM, and a policy decision selects an innerlay (A, B, or C); here assume A is selected. X's PRM knows the source address of the encapsulation (A:x), but not the address of the destination address, where the packet must egress innerlay A to arrive at Y's PRM. In this case, A's PRM needs an ARP-like

table, but because innerlays are multihop, it is not feasible to use ARP-like broadcast to discover it. The solution is a combination of ARP-like encapsulation based on a table loaded by a BGP-like protocol; we call this *BARP*.

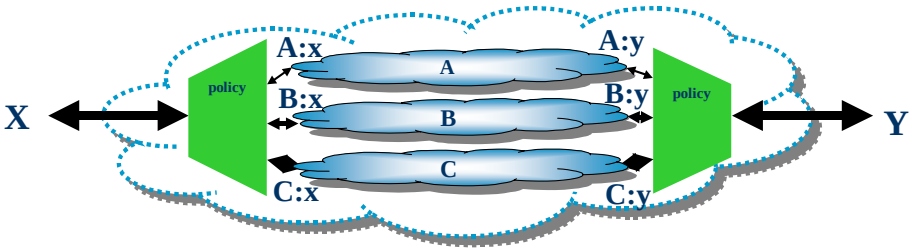

Figure 3. Ingress and egress addresses used to encapsulate packets to traverse sub-overlays

BARP is an indication of how overlays combine properties of network and link layer protocols. In this case, a network-layer transit protocol is used to load a link-layer (pseudo-link, or virtual link here) encapsulation table.

X-Bone modifications

The X-Bone overlay deployment system that underlies the DynaBone was revised to support native recursion. The current DynaBone recursion is supported using the application deployment capability [25][26]. Native support is required for advanced DynaBone capabilities.

The X-Bone control messages (**`x-bone-ctl`**, port 265) were revised to a format similar to that used for the API (**`x-bone-api`**, port 2165). The functions of the OM and RD have been integrated into a single module. Redundant fields were removed, and the language regularized using XML [1]. All management connections are now TCP/SSL, in response to Red-Team security analysis.

The deployment protocol was revised to support more robust recursive deployment of multi-layer overlays. The protocol now includes two recursive phases – a *discover* phase and a *configure* phase. The discover phase is itself composed of three component phases – *invite*, *select*, and *commit/release*. The resulting protocol is under analysis and implementation will ensue in the future release of X-Bone.

The X-Bone API has been augmented to allow arbitrary graphs to be specified, and the web GUI extended to allow those topologies to be entered by reference to a URL, either local (file://), other external (ftp:// or http://). The GUI translates the topology graph into an X-Bone-API-compliant netlist. When topologies are specified using static routing, a default routing table is computed by the Overlay Manager prior to overlay deployment. The use of these netlists allows arbitrary topologies.

Controllable in-kernel multiplexer

The initial PRM was developed as a custom, configurable Perl module [2], and was useful for testing the modular architecture and API, but its performance was poor, near 128Kbps on a dual 2.4Ghz Xeon FreeBSD PC. The Netgraph [9] version, implemented

inside the kernel and in compiled code, achieved near IP-forwarding (300K pkts/sec) bandwidths. This version has additional multiplexing policies and a full control interface, including a *SVG*-based [6] web front-end to visualize and control the PRM. The PRM was also integrated with the *Snort* [16] intrusion detection system, to detect both in- and out-of-band attacks.

The PRM is composed of a core module (PRM), and the following component modules:

- MUX: the packet multiplexer, itself utilizing a set of multiplexing algorithms, including round-robin, see-saw, random, and copy (replication)
- BARP: the interlayer address resolution and border gateway redirection mechanism, key to supporting recursive overlays
- IFACE: manages the *divert* sockets [4], *ipfw* [7] rules, IP-in-IP [11] implementation, and *tun* devices [24].
- API: control and monitoring interface, including a simple web server

The API provides a simple set of interface commands:

- /data — return packet history (see below for format)
- /policy — return current muxing policy
- /policy?policy=<p> — set current muxing policy
- /stop?innerlay=<x> — signal innerlay <x> is under attack
- /go?innerlay=<x> — signal innerlay <x> is NOT under attack

The packet history returned by /data is a format specified by an EBNF. The API also provides SVG code to interpret the returned data format, including a GUI showing which innerlays are in use and the packets on them, and disables/enables innerlays via key clicks.

A number of multiplexing policies were implemented, including per IP-packet random (pick an innerlay at random), and transport-protocol per IP-packet (TCP over one innerlay, UDP over another, other transport protocols over a third). The PRM also supports policy replacement and dynamic policy modification, both in support of dynamic passive restoration.

2.3 Performance Measurements

Detailed measurements of the performance of various dimensions of the DynaBone were performed. These include detailed measurements of the *Netgraph* implementation of the PRM (multiplexer), as well as measurements of the overheads of recursive overlays and large numbers of concurrent innerlays.

Preliminary measurements indicate that the PRM can achieve approximately 45% of the packets/second forwarding performance of a conventional PC-based gateway. In Figure 4, the upper line shows conventional IP forwarding performance, and the lower shows the PRM. Figure 5 shows the same values plotted as Mbps, correcting for the additional header overhead of the PRM, which uses two-layers of IP headers. The overall performance reaches near 85% of line rate of a gigabit Ethernet interface for conventional Ethernet MTUs.

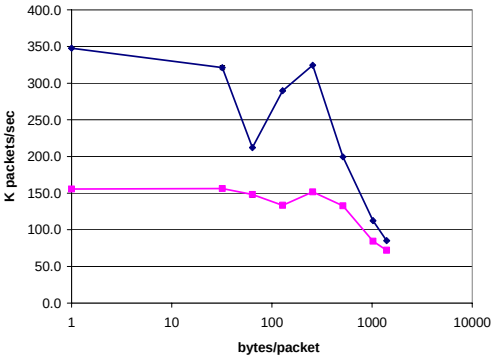

Figure 4. Forwarding performance of the PRM (lower) and conventional IP (upper)

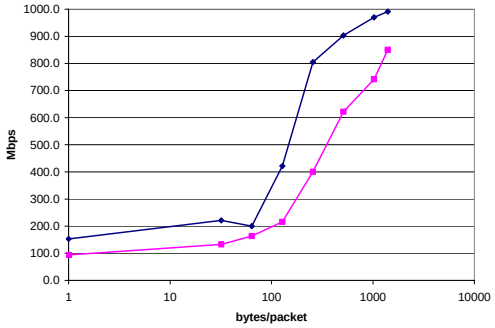

Figure 5. Sustained throughput of the PRM (lower) and conventional IP forwarding

The DynaBone with PRM is a two-layer overlay, achieving 155K packets/sec sustained forwarding performance (Figure 4). Figure 6 shows the forwarding performance of various numbers of encapsulation headers, i.e., various numbers of levels of recursive overlays. Note that the DynaBone, corresponding to a 2-layer overlay with an additional PRM, has nearly the same performance of a general 2-layer overlay. (NB: different lines in Figure 6 represent the performance of different packet sizes).

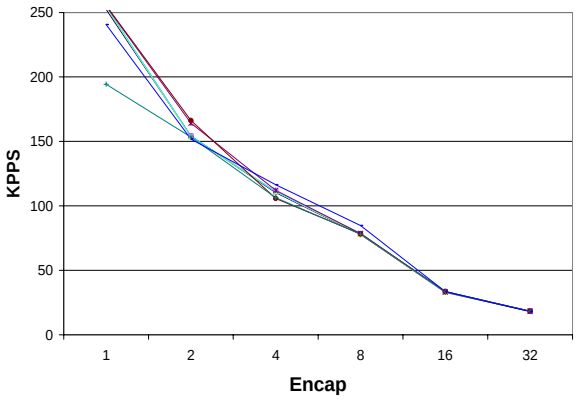

Figure 6. Forwarding performance of layers of recursive overlays

The overall performance of IPsec was also measured on the more recent hardware, to determine what kinds of performance could be expected from the DynaBone in the presence of encryption and authentication. Baseline experiments of various IPsec encryption (none, DES, 3DES) and authentication (none, MD5, SHA1) were performed both between hosts (solid bars) and through an intermediate host-based router (designated "-R", and shown in stripes). Figure 7 compares the performance of these algorithms on a system without any tunneling, using 1-byte packets, and measured the packets/second throughput.

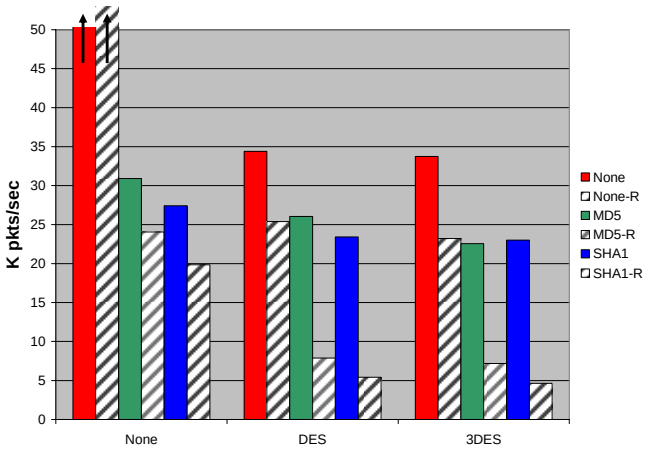

Figure 7. Preliminary IPsec throughput

Throughput of an unencrypted system goes far off the chart, around 350 K packets/sec. Rates through routers drop compared to host-to-host throughput by approximately 25% for systems using only authentication or encryption alone. The forwarding drop is more substantial – 70-80%, vs. the expected 50% cumulative effect – when authentication and encryption are combined.

The throughput of encryption was measured as the packet size varied, from 1 byte through 512 bytes (Figure 8). The performance for both DES and 3DES drops substantially after an initial plateau of 1-32 bytes; this may be an effect of the data cache

or cache line size. The drop in throughput for reasonable payload sizes is substantial, even on dual-processor 2.4 GHZ Xeon machines running FreeBSD.

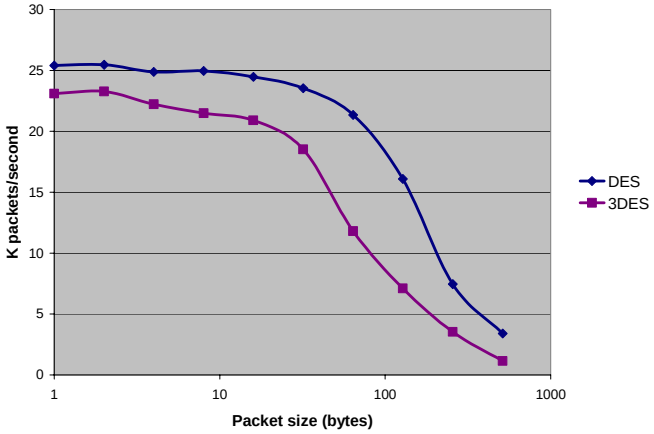

Figure 8. IPsec throughput vs. packet size

Further performance tests were conducted to compare various encapsulation and IPsec algorithms in the X-Bone (single-layer overlay) and DynaBone (two-layer overlay). Measurements were conducted for various configurations of <encryption, authentication> pairs, as shown in Figs. 1-4. For DynaBone, the distinct performance variations remain significant, i.e., to distinguish the characteristics of various innerlay configurations.

Figure 9 shows the bandwidth of various configurations, including no IPsec (top curve), using polling-based communication. It is notable that even high-performance systems (dual 2.4 Ghz Xeon processors with high-speed RDRAM) still show substantial performance penalties for invoking even the simplest IPsec algorithms. The impact ranges from 30-90% of no-IPsec throughput.

Figure 10 shows the comparative packet rates for the various algorithms. Here it is somewhat notable that the performance curves cross, in particular for DES and 3DES, where the performance penalty of these algorithms is more substantial as the packet size grows. This might occur because DES and 3DES do not pipeline or further optimize for large packets, or because they incur a higher cache thrashing penalty than other algorithms.

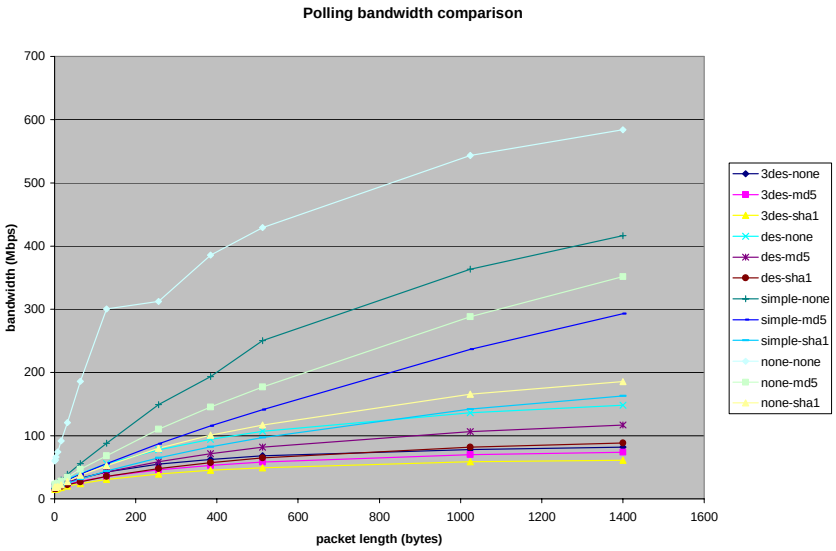

Figure 9. Bandwidth of various IPsec algorithms tested in DynaBone (polling)

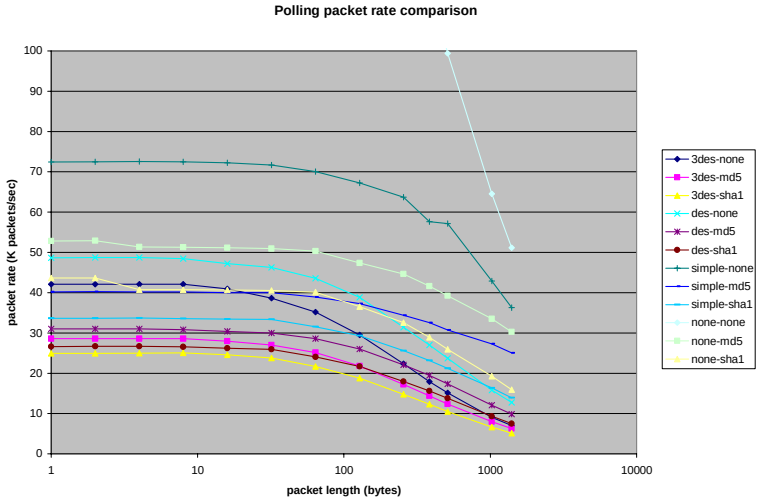

Figure 10. Packet rates of various IPsec algorithms tested in DynaBone (polling)

2.4 TetherNet

Some improvements were made to the TetherNet Internet subnet rental system [17]. The final release of the system included hardware-based cryptography support and fair link bandwidth sharing via FreeBSD Dummynet [15]. Fair sharing ensures that individual users cannot starve others on the rented subnet, and was the last anticipated addition to provide reliable, unattended support for PI meetings. Support for 802.11b wireless (including 128-bit WEP), as well as hardware IPsec encryption were added.

A TetherNet box has been loaned to John Drake (Schafercorp), to support local DARPA meetings, as well as being brought by DynaBone staff to PI meetings and demos at other DARPA-sponsored events. Arrangements for ongoing support for the TetherNet system

are underway, and it is expected to be an offered service of Los Nettos (the regional Internet consortium in Los Angeles managed by USC/ISI) shortly. TetherNet also supported demos at the DARPA Active Networks Conference and Exposition (DANCE), the University College of London (UCL) and the Aerospace Corporation, SPAWAR, and various NSF and DARPA PI meetings.

3. Discussion of Established Targets

The contract start for this project was June 1, 2001; work began immediately after the contract was negotiated, commencing on August 8, 2001. Project progress is tracked from the August date.

The project completed a preliminary implementation of the PRM ahead of schedule, and demonstrated the PRM and innerlays at the DARPA FTN PI Jan 2002 meeting on schedule. Passive restoration of innerlays was demonstrated at the DARPA FTN PI meeting in July 2002, on schedule. Manual reconstitution and automated access reconstitution were demonstrated at the FTN PI meeting in Jan. 2003, using web-based control of the PRM. Separate innerlays were demonstrated since the Jan. 2002 demos, and the system supports 800 separate innerlays. The DARPA FTN PI meeting July 2003 demo showed a high-performance in-kernel PRM, as well as integration with an automated attack detection tool, again on schedule. The final release of the X-Bone software suite, v3.0 in Jan. 2004, supported physically-separate innerlays are by using explicit invitation lists, on schedule.

4. Publications

Y. Wang and J. Touch, “Similarities Between Virtual Networking and Virtual Memory,” (in preparation).

J. Touch and Y. Wang, “Architectural Principles of Virtual Networking,” (in preparation as a research paper).

Y. Want and J. Touch, “Interpretation of PPVPN Framework and Requirements in the Context of the Internet Architecture,” (in preparation as an Internet Draft).

Touch, J., et al., “Using Parallel Overlays for Fault Tolerance in the DynaBone,” (in preparation as a research paper).

Finn, G., et al., “An API for Deploying Layered Overlays,” (in preparation as a research paper,).

Touch, J., Wang, Y., Eggert, L., Finn, G., “Virtual Internet Architecture,” Presented at the Future Developments in Network Architecture (FDNA) Workshop at SIGCOMM, August 2003. ISI Tech. Report ISI-TR-2003-570, http://www.isi.edu/touch/pubs/isi-tr-2003-570

Touch, J., Eggert, L., Wang, Y., “Use of IPsec Transport Mode for Dynamic Routing,” Internet Draft, updated Sept. 2003 (submitted as an Informational RFC).

Touch, J., Finn, G., Wang, Y., Eggert, L., “DynaBone: Dynamic Defense Using Multi-layer Internet Overlays,” Proc. 3rd DARPA Information Survivability Conference and Exposition (DISCEX-III), Washington, DC, USA, April 22-24, 2003, Vol. 2, pp. 271-276.

Touch, J., Eggert, L., Wang, Y., “TetherNet Anti-NAT - Secure Internet Subnet Rental System,” Proc. 3rd DARPA Information Survivability Conference and Exposition (DISCEX-III), Washington, DC, USA, April 22-24, 2003, Vol. 2, pp. 112-114.

Wang, Y., Touch, J., Finn, G., Eggert, L., “An API for Describing and Deploying Virtual Networks,” Nov. 2002 (in prep. as ISI tech. report).

Touch, J., “Those Pesky NATs,” IEEE Internet Computing, July/August 2002, p. 96.

Touch, J., Eggert, L., Wang, Y., “An Architecture for Layer 3 Virtual Networks,” Internet Draft, June 2002.

Touch, J., Wang, Y., Eggert, L., “Virtual Internets,” June 2002, ISI Technical Report ISI-TR-2002-558.

Touch, J., Hughes, A., Wang, Y., Eggert, L., “The ISI Summer Graduate Research Experience Program,” August 2002, ISI Technical Report ISI-TR-2002-563 (In participants proceedings, 2002 Sigcomm Education Workshop).

Touch, J., Wang, Y., Eggert, L., “Virtual Internets for Lab and Class Experiments,” August 2002, ISI Technical Report ISI-TR-2002-562 (In participants proceedings, 2002 Sigcomm Education Workshop).

Wang, Y., Touch, J., “Issues in Link Addressing Support for Layered Virtual Networks,” (in preparation as an Internet Draft).

Wang, Y., Touch, J., “Application Deployment in Virtual Networks Using the X-Bone,” Proc. DANCE: DARPA Active Networks Conference and Exposition, May 2002, pp. 484-493.

Yoon, S., et al., “A Summary of Network Layer Striping Techniques,” (internal report).

5. Personnel

Project Leader: Joe Touch

Research Scientists: Greg Finn

Graduate research assistants:

- Lars Eggert (Jun 01 – Dec 03)
- Amy S. Hughes (Jun 01 – Dec 02)
- Nimish Kasat (Jan 03 – Dec 03)
- Yu-Shun Wang
- Sun-Hee Yoon (Jun 01 – Dec 02)

6. Presentations

Joe Touch and Yu-Shun Wang attended the DARPA FTN PI meeting in Colorado Springs, CO, July 30 - Aug. 2, 2001. There they gave a talk on the DynaBone. There they met with Peter Reiher (UCLA) and Bob Kaminski (AFRL) regarding collaboration.

Joe Touch and Lars Eggert attended the IETF in London, U.K., Aug. 6-10, 2001. There they participated in the IPsec, PPVPN, Multi6, and Transport working groups advanced issues in overlay network architecture.

Joe Touch attended Opticomm 2001 in Denver, CO, Aug. 20-22, 2001.

Joe Touch, Lars Eggert, Yu-Shun Wang, and Amy Hughes attended Sigcomm 2001 in San Diego, CA, Aug. 27-31, 2001. There they met with a number of faculty, notably from the UC system (UCSD, UCB, UCLA, UCSC, UCI) regarding upcoming visits to present initial work on the DynaBone.

Peter Reiher, UCLA, visited ISI on Sept. 20, 2001, regarding potential collaboration between UCLA, the Aerospace Corporation, and the DynaBone project.

Joe Touch attended the IEEE Computer Communication Workshop on Oct. 15-17, 2001. This travel was sponsored by another project.

Peter Reiher, UCLA, and several guests from the Aerospace Corporation visited ISI on Nov. 6, 2001, regarding potential collaboration with the DynaBone project.

Joe Touch attended the IEEE Infocom 2002 TPC meeting in NY, NY, on Nov. 10, 2001. During a later part of that trip, on Nov. 17, 2001 in Philadelphia, PA, he visited with Roch Guerin's students in the EE Dept. of the University of Pennsylvania, and gave a presentation on DynaBone.

Joe Touch gave an invited presentation at UC Berkeley on Nov. 19, 2001, on the DynaBone. There he met with Darleen Fisher and Ion Stoica regarding potential collaboration.

Joe Touch met with Edmond Jonckhere and his students at USC's main campus on Nov. 30, 2001, where he also gave a presentation on the DynaBone.

Joe Touch attended the DARPA Active Nets PI meeting in Orlando, FL, Dec. 3-5, 2001. There he met with Peter Kirstein regarding collaboration with RadioActive, and discussed uses of the DynaBone's overlay system for A-Bone deployment and emerging interest in active overlay networks.

Joe Touch gave an invited presentation at UCLA on Dec. 6, 2001, on the DynaBone. There he met with Mario Gerla to discuss potential collaboration.

Joe Touch, Lars Eggert, and Yu-Shun Wang attended the IETF in Salt Lake City, UT, on Dec. 10-14, 2001. There they gave a presentation in the IPsec WG on IP-VPN compatible IPsec tunnel configuration, and met with an informal group to discuss a sub-WG on layer 3 PPVPNs.

Joe Touch and Yu-Shun Wang attended the DARPA FTN PI meeting in San Diego, CA, on Jan. 15-18, 2002. Joe gave a presentation on DynaBone, and Joe and Yu-Shun provided automated Internet tunneling via the "TetherNet" system.

Joe Touch attended the WIDE workshop in Palo Alto, CA, on Jan 25, 2002. There he met with Jun Murai (Chair, WIDE Project) and Larry Landweber (Univ. Wisconsin) regarding potential collaboration.

Lars Eggert and Y-Shun Wang attended an Internet-2 IPv6 Workshop Feb. 11-12, 2002, at ISI.

Joe Touch participated in an NSF panel on Feb. 12-13, 2002, in Alexandria, VA. His participation was sponsored by the NSF.

Joe Touch and Yu-Shun Wang attended the IETF in Minneapolis, MN, Mar. 18-22, 2002. Joe gave a presentation on routing support for IPsec tunnels in the IPsec WG. Joe and Yu-Shun participated in a meeting of the IPsec CE-PPVPN design team, and participated in the general PPVPN WG meeting. Joe also participated in the L2-Triggers BOF session.

Joe Touch attended the Workshop on Protocols for High-Speed Networks in Berlin, Germany, on April 22-24, 2002. Joe gave a presentation on Peer Networks - High-Speed Solution or Challenge? As part of this trip, he met with Peter Kirstein and his research group at the University College London to discuss collaboration on an upcoming demo (DANCE).

Joe Touch and Yu-Shun Wang attended the DARPA Active Networks Conference and Exposition (DANCE) in San Francisco, CA, on May 28-30, 2002. There they gave a

demo of the TetherNet system, and discussed collaboration on DynaBone with attendees. TetherNet was used to support the demos for this meeting.

Joe Touch met with Doug Maughan and Nick Lomberos of DARPA on June 17, 2002, to discuss the use of the TetherNet system to support DARPA PI meeting demos, as well as larger-scale demos.

Joe Touch attended Infocom in NYC, NY, June 24-27, 2002. There he participated in a meeting of the IEEE Technical Advisory Committee (TAC), representing the Internet Technical Committee (ITC), which he co-chairs, as well as the planning meeting for the TPC for Infocom 2003. He also met with Darleen Fisher of UC Berkeley, David Sincoskie of Telcordia, Nadia Shalaby of Princeton, Carl Gunter of Univ. Pennsylvania, and others regarding potential collaborations with DynaBone.

Joe Touch, Lars Eggert, and Yu-Shun Wang attended the 54th IETF in Yokohama, Japan, on July 15-19, 2002. There they participated in IPsec, PPVPN, and Transport-area WG meetings, and met with a number of participants, notably Mark Duffy of Quarry Technologies and Greg Lebovitz of Netscreen.

Joe Touch and Lars Eggert attended the DARPA FTN PI meeting in Newport, RI, July 23-26, 2002. Joe gave a presentation on DynaBone, and they both gave a demo of the DynaBone system. The demos for the entire PI meeting, as well as those for the DARPA DC PI meeting the week before, were supported using the Tethernet.

Joe Touch attended the Sigcomm 2002 conference in Pittsburgh, PA, Aug. 20-23, 2002. As Secretary/Treasurer of the Sigcomm SIG, he participated in a number of organizational and planning meetings, as well as reporting to the SIG membership.

Joe Touch attended a USC workshop on technology transfer in San Diego, CA, Sept. 24, 2002. There he gave a presentation on the TetherNet system.

Joe Touch and Lars Eggert attended the DARPA FTN PI meeting in San Antonio, TX, on Jan. 28-30, 2003. Joe gave a presentation on the DynaBone, including a summary of Red-Team analysis of the underlying X-Bone system security, and Lars ran the TetherNet network lease system to support both FTN and DC demos.

Joe Touch, Lars Eggert, and Yu-Shun Wang attended the 56th IETF in San Francisco, CA, on Mar. 17-20, 2003. There they participated in IPsec, PPVPN, Transport-area, Sub-IP meetings, and met with a number of participants.

Joe Touch attended Infocom 2003 in San Francisco on Apr. 1-3, 2003. There he participated in an editorial board meeting for Computer Networks journal and various executive committee meetings.

Joe Touch and Yu-Shun Wang attended DISCEX-3 in Alexandria, VA on Apr. 22-24, 2003. There they gave a demo of the TetherNet Internet subnet rental system, and used the TetherNet to support 60 demos.

Joe Touch attended a meeting of the International Collaboration Board (ICB) in Alexandria, VA on Apr. 25, 2003.

Joe Touch participated in a review of the Interplanetary Internet architecture at ISI in Marina Del Rey, CA on May 8, 2003.

Joe Touch attended a meeting of the International Collaboration Board (ICB) in London on July 10-11, 2003. There he met with Peter Kirstein of UCL and gave a presentation on the DynaBone system, which is under consideration for use by the ICB for a pan-European testbed.

Joe Touch and Lars Eggert attended the 57th IETF in Vienna, Austria on July 14-18, 2003. Joe participated in meetings of the L3VPN WG, as well as participating in meetings with various WG chairs and Area Directors regarding the revision of Internet Drafts he co-authored.

Lars Eggert gave an invited presentation on "Virtual Internets" at NEC Network Labs, Heidelberg, Germany, on July 22, 2003. There he met with Heinrich Stüttgen, Amardeo Sarma, Jürgen Quittek, Marco Liebsch, and Marcus Brunner. Travel for this meeting was partly provided by NEC.

Joe Touch and Yu-Shun Wang attended the DARPA FTN, DC, and CONE PI meetings in Honolulu, HI, on July 20-25, 2003. Joe gave a presentation on the DynaBone project, and Joe and Yu-Shun provided Internet access for the combined demos of all three PI meetings using the TetherNet Internet subnet rental system.

Lars Eggert gave an invited presentation on "Virtual Internets" at the University of Tübingen, Tübingen, Germany, on July 25, 2003. There he met with Georg Carle, Gerhard Münz, and Egbert Fridrich.

Joe Touch attended Sigcomm 2003 in Karlsruhe, Germany on August 25-29, 2003. As outgoing ACM SIGCOMM Treasurer and incoming SIG Conference Coordinator, Joe participated in various executive committee meetings. Joe attended the Workshop on the Future Developments in Network Architecture co-located with Sigcomm 2003, and presented a paper on the "Virtual Internet Architecture," based on the X-Bone/DynaBone architectures.

Lars Eggert gave an invited presentation on "A Virtual Internet Architecture" at the British Telecom Edge Lab, Ipswich, UK, on September 2, 2003. There he met with Bob Briscoe, and Peter Hovell. Travel for this meeting was provided by British Telecom.

Joe Touch attended HotNets-I in Princeton, NJ, on Oct 28-29, 2003. As part of that trip, he met with Carl Gunter on Oct 25, 2003 in Philadelphia, PA, at the University of Pennsylvania, where he gave an invited talk on the DynaBone.

Joe Touch, Lars Eggert, and Yu-Shun Wang attended the 55th IETF in Atlanta, GA, on Nov. 18-21, 2003. There they participated in IPsec, PPVPN, Transport-area, Sub-IP meetings, and met with a number of participants, notably Steve Kent of BBN, Mark

Duffy of Quarry Technologies, Paul Knight of Nortel, Hugh Daniel of FreeS/WAN, and Lixia Zhang of UCLA.

Lars Eggert deployed the TetherNet network lease system at a meeting at DARPA/Shaeffer Corporation on Nov. 21, 2003 in Arlington, VA.

Amy Hughes participated in the PlanetLab meeting in Boston, MA, on Dec. 8, 2003. There she presented information on the X-Bone and DynaBone systems, in anticipation of their integration into the PlanetLab infrastructure.

Joe Touch and Yu-Shun Wang attended the 58th IETF in Minneapolis, MN on Nov. 10-12, 2003. They participated in meetings of the L3VPN WG, as well as participating in meetings with various WG chairs and Area Directors regarding the revision of Internet Drafts they co-authored.

Joe Touch gave a presentation at IWAN in Kyoto, Japan on Dec. 10-12, 2003 on related methods to support peer (P2P) application-controlled routing a DynaBone network-layer overlay.

Joe Touch met with Tim Gibson at DARPA in Arlington, VA on Dec 18, 2003, to discuss the progress of the DynaBone system and potential impact on the emerging Control Plane program.

7. Consultative and Advisory Functions

There were no applicable functions performed during this report.

8. New Discoveries

During the second quarter (Oct-Dec01) a new technique for determining encapsulation addresses for forwarding across link and pseudo-link clouds (BARP) was developed.

In the third quarter (Jan-Mar02) a new method was developed for explaining how routers handle tunneled packets internally; this method explains both how existing VPN routers process packets, as well as how to recursively define a VPN as a router.

During the fourth quarter (Apr-Jun02) a new method was developed for explaining how routers handle tunneled packets internally; this method explains both how existing VPN routers process packets, as well as how to recursively define a VPN as a router.

In the Jul-Sep02 quarter a provisional patent was filed for the TetherNet system.

During the Jul-Sep 03 quarter a patent was filed on the TetherNet Internet subnet rental system this quarter, based on a provisional filing in August 2002.

During the Oct-Dec 03 quarter a provisional patent was filed on a new self-configuring tunnel handshake protocol for the TetherNet Internet subnet rental system this quarter.

9. References

[1] Bray, T., Paoli, J., Sperberg-McQueen, C. M., Maler, E.,. *Extensible Markup Language (XML) 1.0 (Second Edition).* **W3C Recommendation,** October 6, 2000.

[2] CPAN Perl module library, http://www.cpan.org/

[3] Deering, S., Hinden, R., "Internet Protocol, Version 6 (IPv6) Specification," RFC-2460, Dec. 1998.

[4] Divert sockets, http://www.anr.mcnc.org/~divert/index.shtml

[5] DynaBone, http://www.isi.edu/dynabone

[6] Ferraiolo, J., (ed.) "Scalable Vector Graphics (SVG) 1.0 Specification," http://www.w3.org/TR/SVG/

[7] IPFW on FreeBSD, http://www.freebsd.org/

[8] McCanne, S., Jacobson, V., "The bsd packet filter: A new architecture for user-level packet capture," Winter USENIX Conference, pp. 259-269, January 1993.

[9] Netgraph, http://www.daemonnews.org/200003/netgraph.html

[10] Patterson, D., Gibson, G., Katz, R., "A case for redundant arrays of inexpensive disks (RAID)," Proceedings of the ACM-SIGMOD International Conference on Management of Data, pp. 109-116, Chicago, IL, June 1988.

[11] Perkins, C., "IP Encapsulation within IP," RFC-2003, Oct. 1996.

[12] Plummer, D., "An Ethernet Address Resolution Protocol - or - Converting Network Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware," RFC-826, November 1982.

[13] Postel, J., (ed.), "Internet Protocol," RFC-791, Sept. 1981.

[14] Rekhter, Y., Li, T., (eds.), "A Border Gateway Protocol 4 (BGP-4)," RFC-1771, March 1995.

[15] Rizzo, L., *Dummynet: A simple approach to the evaluation of network protocols*, ACM Computer Communication Review, Vol. 27, No. 1, pp. 31-41, 1997.

[16] Snort, http://www.snort.org/

[17] TetherNet, http://www.isi.edu/tethernet

[18] Touch, J., "Dynamic Internet Overlay Deployment and Management Using the X-Bone," Computer Networks, July 2001, pp. 117-135.

[19] Touch, J., Eggert, L., Wang, Y., "An Architecture for Layer 3 Virtual Networks," Internet Draft, June 2002.

[20] Touch, J., Eggert, L., Wang, Y., "TetherNet Anti-NAT - Secure Internet Subnet Rental System," Proc. 3rd DARPA Information Survivability Conference and Exposition (DISCEX-III), Washington, DC, USA, April 22-24, 2003, Vol. 2, pp. 112-114.

[21] Touch, J., Finn, G., Wang, Y., Eggert, L., "DynaBone: Dynamic Defense Using Multi-layer Internet Overlays," (to appear in Discex participants' proceedings).

[22] Touch, J., Hotz, S., "The X-Bone," Proc. Global Internet Mini-Conference at Globecom, Nov. 1998.

[23] Touch, J., Wang, Y., Eggert, L., “Virtual Internets,” (submitted to ACM HotNets Workshop).

[24] Tun devices FreeBSD man page, http://www.freebsd.org/

[25] Villanueva, O. A., Touch, J., “Web Service Deployment and Management Using the X-Bone,” Spanish Symposium on Distributed Computing, SEID2000, Sept. 25-27, 2000, Ourense, Spain. http://www.isi.edu/touch/pubs/seid2000.pdf

[26] Wang, Y., Touch, J., “Application Deployment in Virtual Networks Using the X-Bone,” Proc. DANCE: DARPA Active Networks Conference and Exposition, May 2002, pp. 484-493.

[27] X-Bone, http://www.isi.edu/xbone

All references available on the DynaBone website: http://www.isi.edu/dynab